INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 2, Issue 3 OCT 2014

IMPLEMENTATION OF TPA FOR SECURED CLOUD STORAGE DATA

[1] MURALI KRISHNA, [2] HEMANTHA RAMA

[1] M.Tech Student, Department of CSE,

muralik618@gmail.com

[2] Assistant Professor, Department of CSE,

ckhemantha@gmail.com

ABSTRACT— Cloud computing is the arising technology to minimize the utilizer burden in the updating of data in business utilizing internet. Instead of local data storage and maintenance, the utilizer is availed with the cloud storage so that the utilizer can remotely store their data and relish the on-demand high quality application from a shared pool of resources. The data stored must be forfended in the cloud storage. The security challenges cloud computing presents the encumbrance of local data storage and maintenance. Public auditability for cloud data storage security is of critical paramountcy so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an efficacious third party auditor to check the integrity of outsourced data. To securely introduce an efficacious TPA, the auditing process should bring in no incipient susceptibilities towards utilizer data privacy, and introduce no supplemental online burden to utilizer. In this paper, we propose a secure cloud storage system fortifying privacy-preserving public auditing. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Index Terms — TPA, Security, Privacy, Cloud Storage, Data Integrity, Shared Data

I INTRODUCTION

In cloud computing and storage, users are able to retrieve and to sharing resources provided by cloud accommodation vendors at low cost. It is regular activity for users to hold cloud storage accommodations to distribute data with others in a group of people, as data sharing becomes efficient feature in most cloud storage presenting, including Drop box, iCloud and Google Drive. Cloud is a sizably voluminous amount of group of coupled computers, which is a mainly transmuting in how we maintain data and run application. Cloud computing is a shared pool of group of coupled computing resources, whenever we optate we will directly retrieve and provisioned by the accommodation provider. The advantages of cloud are preserving cost. The major drawback of cloud computing is security. Present days Cloud is utilizing so many software companies. Since the security it is a main threat right now withal not provided in cloud, so many industries adopt their individual security. The information maintain place in the cloud is accessable to everyone and any time, security is not at sure. To maintain security of data, cryptographic techniques cannot be accepted directly. Sometimes the cloud vendor may bulwarked the data corruptions to maintain the reputation. To overcome this quandary, we propose an efficient third party auditor to audit the user's outsourced data when needed.

How to enable a bulwarking privacy third-party auditing, unique to data encryption, is the facing major quandary we are going to implement in this paper. Our initial implementation is work among the first few ones to

- acceptance to give forfending privacy from public auditing in cloud, with focusing on information storage. Besides, with the prevalence of cloud computing, a prognosticable growing of auditing work from number of users may be delegated to Third Party Auditing. As the unique auditing of these incrementing tasks can be tedious and cumbersome, a natural demand is then how to enable the TPA to good perform different auditing tasks in a group manner, i.e., parallel. To give solution for these quandaries, our work utilize the technique of public key-predicated homomorphic linear authenticator it enables TPA to perform the auditing without focusing the local facsimile of information and thus greatly reduces the communication and computation overhead as compared to the direct data auditing methods. By coalescing the HLA with arbitrary masking, our approach give confidence that the TPA could not learn any cognizance about the data stored in the cloud computing server during the efficacious auditing process. Aggregation and algebraic properties of authenticator after it will give more advantageous to our development of batch auditing. Specifically, our contribution can be outline as the following three approaches: We amend the public auditing system of information storage security in cloud computing technology and provide a privacy auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.
- To the best of our erudition, our scheme is the first to fortify scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.
- We prove the security and estimate the performance of our developed schemes through concrete experiments and comparisons with the state of the art.

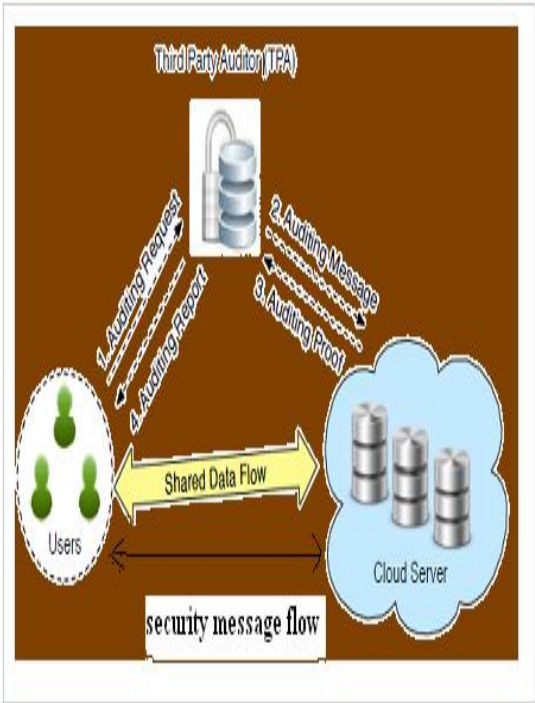

Figure: The architecture of cloud data storage service.

II DESIGN GOALS

The privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should follow the security and performance.

Public Audit: It sanctions TPA to verify the correctness of the cloud data on demand without retrieving a replica of the whole data.

Storage Consistency: the data in cloud server that can pass the audit from TPA without indeed storing users' data intact.

Privacy-Preserving: to ascertain that there subsists no way for TPA to derive users' data content from the information accumulated during the auditing process.

Batch Auditing: It enables TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly astronomically immense number of different users simultaneously.

Light Weight: It sanction TPA to perform auditing with minimum communication and computation overhead.

III RELATED WORK

Cognate works were carried out by Yan Zhu et al. about the data which the utilizer puts into the cloud will be sent to the Cloud Accommodation Provider(CSP) and a facsimile of it is withal sent to the Third Party Auditor (TPA) which checks for the correctness of the data. Dynamic audit accommodation is done for verifying the integrity of un-trusted and outsourced storage. Here periodic sampling is done to minimize the computation cost of TPA and storage accommodation provider.

The cognate works carried out by Qian Wang et al. studied that so as to ascertain the credibility of the data that is being used during the auditing process a remote integrity checking protocol is utilized. This protocol is opportune for integrity aegis of the data stored in cloud. It fortifies dynamic operations like insertion, effacement and updation of data. To achieve efficient data dynamic, and to amend the storage by manipulating the classic merkle hash tree for block tag authentication.

Further Nandeesh et al. carried out future work on the physical possession of the outsourced data in cloud computing storage engenders incipient security jeopardy. To secure TPA predicated storage utilizing homomorphic tokens and distributed erasure coded data, which sanction to audit the cloud storage with minimum computation cost. To achieve efficient data dynamic operations, we ameliorate the storage on outsourced data including data modification, effacement and updation. To provide redundancy parity vector and guarantees data dependability utilizing erasure-rectifying code in the distribution preparation.

Mururalikrishnan Ramane et al. studied further about the public auditing schemes are utilized efficiently in auditing the data stored in cloud, it solves the issue of restricting TPA to access of the data openly. This scheme verifies the metadata rather than authentic data which provides secure cloud storage that fortifies privacy preserving public auditing. Dalia Attas et al. studied further on cloud computing to ascertain the integrity of the data stored in the cloud storage, TPA fortified with digital signature is used for efficient auditing. This doesn ' t affect the pristine data and additionally audits without injuctively authorizing local facsimile of data. Checking is done in the cloud accommodation provider (CSP) and TPA. The digital signature first performs hash function utilizing message-digest algorithm (MD5). Compute encryption with private key on the other hand decryption by utilizing public key with hash value containing reverse order of its pristine data.

IV PROPOSED SYSTEM

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of major importance to approve public auditing service for cloud computing information storage, so that users may resort to a unique third party auditor (TPA) to audit the outsourced data whenever we needed. The Third Party Auditing, who has to know more and capabilities that users do not, can sequentially check the integrity of all the information stored in the cloud on behalf of the users, which provides a more easier way for the users to ensure their storage correctness in the cloud computing. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud.

Advantages of Proposed System:

- We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.

- To the best of our knowledge, our scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

- We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

V EXPERIMENTAL RESULTS

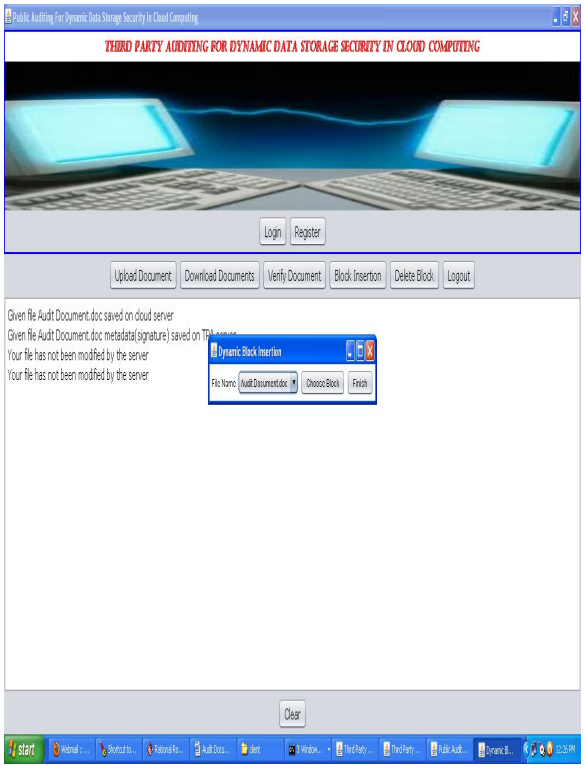

Fig: Block Insertion

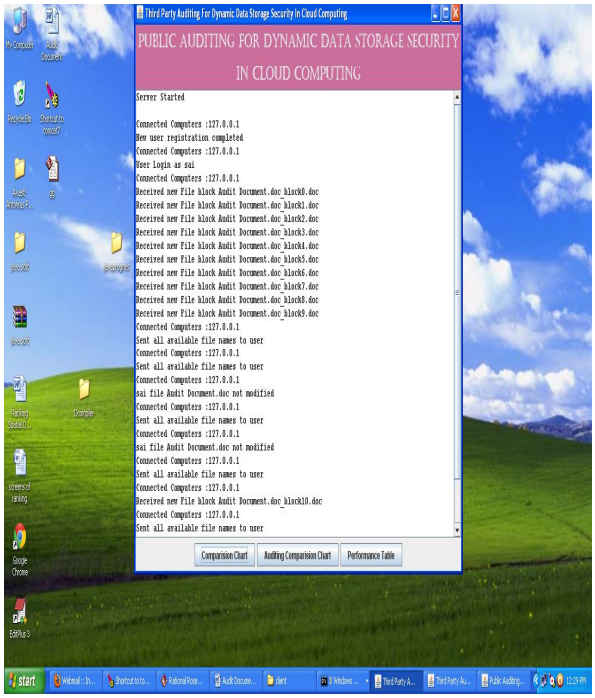

Fig: TPA After all the operation

CONCLUSION

Concluding to this paper, we propose a protecting privacy from public auditing through security storage in cloud computing. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, we explore a Cloud Computing new entity privacy-preserving public auditing system for the purpose of data storage security, where TPA works on auditing details without need of data which was stored locally. Here we uses the authenticator with feature of homomorphism and also using technique random mask to create trust on cloud that used TPA will not get or bother about the information which was stored by the user while auditing process, it also reduces the workflow to cloud user from the annoying and cost efficient auditing task, but also take the edge off the users to decrease the fear of their uploaded data privacy.

FUTURE WORK

Under taking TPA may concurrently handle different audit levels from various users for their updated data files, in

addition we extend our privacy-preserving public auditing protocol from single user to multi-user, here TPA workouts on various number of auditing tasks parallel. Efficient security and performance analysis gives reports that the proposed techniques are secure and highly efficient. The mighty features of the proposed schemes reduce the burden of economies in future for Cloud Computing.

REFERENCES

[1] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, 3-42.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE INFOCOM, 2010, pp. 525–533.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in Proc. European Symposium on Research in Computer Security. Springer-Verlag, 2009, pp. 355–370.

[4] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," University of Toronto, Tech. Rep., 2011. [Online]. Available: http://iqua.ece.toronto.edu/~ bli/techreports/oruta.pdf.

[5] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," in Proc. ACNS. SpringVerlag, 2012.

[6] C. Wang, K. Ren, W. Lou and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[7] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012

[8] Lingaraj Dhabale, Priti Pavale, "Providing Secured Data Storage by Privacy and Third Party Auditing In Cloud",International Conference on Computing and Control Engineering, ISBN 978-1-2248-9, 12 & 13 April, 2012

[9] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. ,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[10] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, "Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security", International Journal of Scientific and Engineering Research, vo. 4, no. 2, ISSN 2229-5518, Feb 2013.

[11] Gayatri. R, "Privacy Preserving Third Party Auditing for Dynamic Data", International Journal of Communication and engineering, vol. 1, no. 1, issue: 03, March 2012

[12] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

[13] Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. 584-59.

[14] Honywei Li, Yuanshun Dai, Bo Yang. "Identity-Based Cryptography for Cloud Security".

[15] C. Hota, S. Sanka, M. Rajarajan, S. Nair, "Capabilitybased Cryptographic Data Access Control in Cloud Computing", in International Journal of Advanced Networking and Applications, Volume 01, Issue 01, 2011.